Transforming the voting process integrating blockchain into e-voting for enhanced transparency and security

Agus Tedyyana[1,2], Osman Ghazali[2], Tryo Asnafi[3], Onno W. Purbo[4], Nur Ziadah Harun[5], Faizal Riza[1]
[1]Department of Informatic Engineering, Politeknik Negeri Bengkalis, Riau, Indonesia
[2]School of Computing, College of School of Arts and Science, University Utara Malaysia, Sintok, Malaysia
[3]Open Source and Open Mind Company, Equnix Business Solutions, Jakarta, Indonesia
[4]Department of Informatic, Institute Technology Tangerang Selatan, Tangerang, Indonesia
[5]Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia, Johor, Malaysia

Article Info

Article history:

Received Oct 9, 2023
Revised Dec 22, 2023
Accepted Jan 12, 2024

Keywords:

Blockchain
E-voting
Security
Smart contract
Transparency

ABSTRACT

This study introduces a novel e-voting system utilizing blockchain technology to address the challenges inherent to traditional voting methods. Traditional systems often suffer from inaccuracies, susceptibility to manipulation, and elevated costs. Conversely, while e-voting shows potential, issues related to transparency and security have curbed its full adoption. Our research overcomes these hurdles by integrating a system developed through the Kanban methodology, with the blockchain serving as the central repository for all election data. This approach boosts transparency and security, using public-private key pairs for each transaction, and simplifying blockchain access. Organizers initiate elections and define eligible voters; this data is then securely moved to the Ethereum blockchain. Voters can effortlessly use the system, casting votes and accessing real-time, unalterable results. Various communication protocols ensure system stability, with simulated cyberattacks showcasing its security. After exhaustive testing and refinement, areas for further enhancement have been identified. This innovative system offers unmatched transparency and trust in the voting process, marking a considerable leap for trustworthy elections, especially in small to medium-sized settings.

Corresponding Author:

Osman Ghazali
School of Computing, College of School of Arts and Science, University Utara Malaysia
Sintok, Kedah, 06010, Malaysia
Email: osman@uum.edu.my

1. INTRODUCTION

Inside the context of modern democracy, the act of voting assumes a crucial significance in shaping collective outcomes, spanning from the selection of national leaders in presidential elections to the appointment of individuals in positions of authority inside organizations. Nevertheless, traditional electoral systems that rely on paper ballots and manual procedures sometimes face a range of difficulties, such as high expenses, complex operating procedures, and the possibility of misconduct [1]. These obstacles have the potential to undermine public confidence in the credibility of election results. The advent of information technology has given rise to the potential of electronic voting (e-voting), presenting a more streamlined and accurate substitute for conventional voting approaches. However, e-voting is not devoid of its array of obstacles, with concerns over transparency, data integrity, and security taking center stage [2]. Blockchain technology has emerged as a potential answer to these difficulties, providing exceptional transparency and security through its decentralized, and distributed ledger capabilities. Furthermore, the use of smart contracts in blockchain technology enables the automation and validation of transaction procedures, guaranteeing that actions taken are by predetermined agreements, thereby eliminating the necessity for involvement from external parties [3].

The objective of this study is to leverage the capabilities of blockchain technology [4], to create a decentralized application for e-voting. By utilizing the Ethereum network and the truffle framework, this study proposes the utilization of smart contracts as self-executing electoral agreements. The design of the Ganache network strengthens the prototype's ability to record voting transactions independently of a central database. This enables voters to verify election results by examining each transaction on the local blockchain [5]. This project endeavors to design a blockchain-based e-voting system by implementing the Kanban development technique [6], which prioritizes disciplined organization and transparent workflow [7]. The primary objective of this system is to improve the transparency and integrity of voting results, while simultaneously addressing the inherent difficulties commonly seen in conventional e-voting systems [8]. The integration of blockchain technology into e-voting systems has the potential to redefine election processes by providing improved security, accountability, and public trust in the democratic system [9]. This development is occurring with the ongoing worldwide digitization and increased scrutiny of democratic procedures.

This research raises crucial inquiries regarding the seamless integration of blockchain technology into e-voting systems. In what ways may blockchain be efficiently integrated into e-voting systems? can blockchain technology serve as a safeguard, guaranteeing the transparency and security of vote outcome data? the objective of this study is to investigate the integration of blockchain technology with e-voting systems, with a focus on developing a comprehensive framework. This framework intends to enhance transparency and strengthen the security of voting result data. This study aims to enhance both academic comprehension and practical utility by examining the fundamental concepts of elections and their integration with e-voting. Furthermore, this study aims to provide insights into the prospective applications of decentralized technology, such as blockchain, within the realm of e-voting systems. An essential element of this study pertains to its emphasis on mitigating unlawful alterations of recorded votes and ensuring the integrity of each individual's democratic expression. The primary objective of this study is to guide future research focused on decentralized data storage systems, to facilitate the harmonious evolution of the democratic process alongside technology improvements.

2. METHOD

The utilization of the Kanban method in the development process of the e-voting system involves the integration of a digital Kanban board provided by the software platform Notion. The Kanban process starts with a 'literature review', followed by tasks being placed in a 'Kanban backlog'. From there, tasks move through the stages of 'to do', 'in progress', 'Testing', and finally 'Done'. After all tasks are completed, the process concludes with a 'Final Report'. Each task progresses sequentially from one column to the next, ensuring a systematic approach to the development work. This structured workflow is designed to optimize efficiency and track the progress of the project until its completion. The subsequent stages outline the intended research on e-voting systems:

The provided diagram, labeled as Figure 1, illustrates the visual representation of the subject matter under discussion. The research process begins with a comprehensive study of existing literature about e-voting and blockchain systems. Subsequently, an examination of the suggested system ensues. The analysis is subsequently represented in the form of a backlog. Tasks that are included in the backlog are assigned specific time limits and are subsequently recorded in the to do column. The process of system development commences with the transition of a task from the "to-do" state to the "in-progress" state. After the assignment has been finished, it is transferred to the Testing column for assessment. After undergoing testing and receiving approval, the work is then moved to the done column, signifying its successful completion.

2.1. Related works

In the domain of health insurance, people and health insurance organizations have enduring obstacles. The aforementioned issues have stimulated the investigation of utilizing blockchain and semantic web technologies to augment the efficacy of smart contracts inside this particular domain [10]. The underlying cause of these issues might be attributed to the divergent methodologies employed in the compensation of injuries arising from clinical trials across different nations. In the United States, the determination of compensation for these injuries is discretionary, whereas in countries such as the Netherlands, it is closely tied to instances of medical misconduct, frequently resulting in legal conflicts. On the other hand, certain nations, such as New Zealand, have implemented a more efficient strategy by providing direct compensation without requiring substantial evidential requirements beyond the documentation of the harm. The fundamental aim of the research project was to devise a transparent, secure, and mutually acceptable system for health contracts that could be readily validated. To accomplish this objective, the researchers developed a decentralized application (DApp) that utilizes the capabilities of blockchain and semantic web technologies [11], [12]. The objective was to enhance the ease, reliability, and legitimacy of agreements between individuals and health insurance entities on their healthcare claims.

The internet-based polling systems were found to have vulnerabilities that rendered them prone to a range of security risks. In response, scholars devised secure and verifiable polling system (SeVEP). The present polling system was developed with the primary objective of safeguarding the rights and privacy of voters, verifying the identities of voters, facilitating the casting of multiple ballots within a certain period, and mitigating instances of duplicate voting. The secure, verifiable, and operationally sound nature of the SeVEP polling system was established through a comprehensive evaluation process that included rigorous security evaluations, performance testing, and comparison analysis [13].

The researchers implemented an e-voting system as a potential remedy for the limitations observed in traditional voting systems. The culmination of their extensive research efforts has resulted in the development of an internet-based software application for electronic voting, referred to as the next generation election e-voting web application. The aforementioned system is characterized by its ability to facilitate remote voting and its commitment to upholding voter privacy, fairness, comprehensiveness, originality, and resilience in the political process [14].

The inadequacies of the centralized system in the context of crowdfunding were emphasized. The development of a decentralized crowdfunding system prototype was undertaken by researchers, who utilized blockchain technology and integrated smart contracts. This application aimed to address the needs of both fundraisers and funders inside crowdfunding systems [15]. In response to the pervasive problem of fraudulent academic credentials, the study proposes a potential remedy through the implementation of a blockchain-based e-transcript system. The objective of this design was to offer a comprehensive set of features including security, transparency, autonomy, anonymity, data integrity, and resilience against distributed denial of service (DDoS) attacks [16].

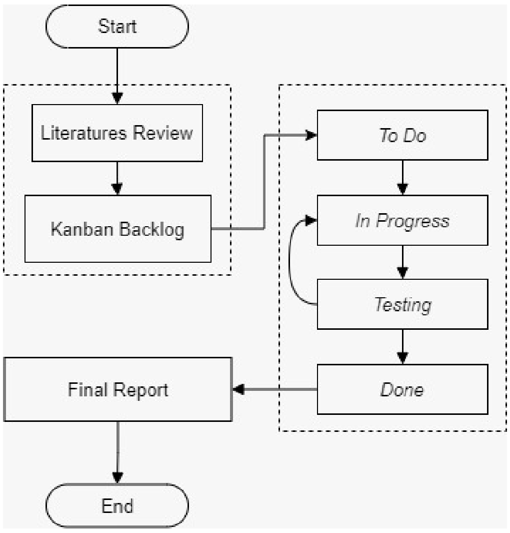


Figure 1. Research stages

2.2. E-voting

The act of voting serves as a crucial means by which individuals determine the individuals who will assume positions of political representation and manage institutions. Utilized in a wide range of contexts, spanning from corporate environments to national arenas, it serves as a highly effective instrument for facilitating democratic decision-making processes. Throughout history, the act of voting has served as a fundamental means for individuals to express their preferences and make choices [17]. E-voting pertains to the contemporary method of employing information technology to streamline the process of voting. The utilization of this approach presents itself as a potentially effective method for addressing the difficulties and unethical actions commonly observed in traditional voting systems. E-voting has several notable advantages compared to traditional voting methods. These include cost-effectiveness, the removal of paper ballots, and the simplicity it provides to voters, who may simply declare their choice by clicking or tapping a screen [18].

2.3. Blockchain

The advent of the Industry 4.0 revolution has expedited a multitude of advancements in the realm of digital technology, among which is the emergence of blockchain technology [19], [20]. The blockchain is a data structure that consists of interconnected blocks, wherein each new block undergoes processing by participants, also known as nodes, within the network of the blockchain. A block consists of three components: a distinct value known as a hash, data, and the hash of the preceding block. The composition of data within a block is contingent upon its specific type. In the Ethereum blockchain, a block encompasses transaction particulars, encompassing information such as the sender's identity, the recipient's identity, the value of the coins involved, transaction fees, and more relevant details. The user has provided a numerical reference without any accompanying text. The concept of blockchain can be characterized as a decentralized and distributed ledger system. It facilitates the communal sharing and recording of knowledge within a community or network. Each member or participant retains a duplicate of this information. Each time a transaction takes place, all members of the group collectively validate the update. The data contained within the blockchain can include various types of information such as transactional records, contractual agreements, user identities, asset quantities, and any other form of digitally storable data. The permanence and immutability of data stored on the blockchain are notable characteristics. Smart contracts govern the execution, validation, recording, and distribution of data entries. These contracts assume the responsibility of third parties through the execution of intricate algorithms, thereby safeguarding the overall integrity of the blockchain. The integration of blockchain technology into the distribution of databases inside the e-voting system has the potential to address concerns related to election fraud and manipulation [3].

Figure 2 illustration of blockchain, highlighting its fundamental characteristics of decentralization, immutability, and cryptographic linkage. Decentralization refers to the distribution of power across multiple parties, rather than being concentrated in the hands of a single entity. This distribution is characterized by the sharing of authority among all players within a network. This practice ensures the continuous availability of services, mitigates the risk of failures, and ultimately cultivates confidence by providing uninterrupted service. In contrast to centralized databases, the blockchain possesses the characteristic of immutability, hence ensuring the preservation of data integrity. The interconnection of data entries is achieved via the utilization of cryptographic ties and digital signatures, while the assurance of their integrity is established through the implementation of hashing algorithms and the utilization of public-private keys. The primary objective of employing blockchain technology is to attain verifiable immutability. In the event of any modifications made to the data, it becomes necessary to recalculate the hash value of the block that contains the revised data, as well as the hash values of all future blocks. This suggests that it is necessary to utilize solely the hash of the most recent block to guarantee the integrity of all data. In the context of blockchain systems, the information included within blocks consists of verified transactions that have been recorded upon their inception. This design guarantees that any attempt to introduce, remove, or modify a transaction within an already confirmed block will be promptly identified [21].

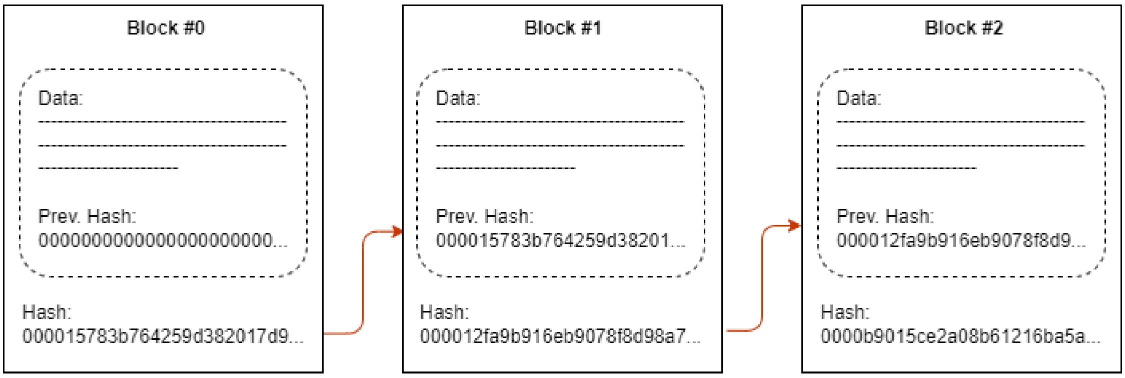

Block #0
Data:
Prev. Hash:
0000000000000000000000...
Hash:
000015783b764259d382017d9...
Block #1
Data:
Prev. Hash:
000015783b764259d38201...
Hash:
000012fa9b916eb9078f8d98a7...
Block #2
Data:
Prev. Hash:
000012fa9b916eb9078f8d9...
Hash:
0000b9015ce2a08b61216ba5a...

Figure 2. Illustration blockchain

2.4. Smart contracts

Smart contracts, also known as digital contracts or self-executing contracts, are computational algorithms that are created to streamline, validate, and implement the conditions of a contract involving several parties, eliminating the requirement for intermediaries or third-party participation. Fundamentally, a smart contract serves as a means to encapsulate the terms and conditions of a contractual agreement between two parties, namely a buyer and a seller. This encapsulation is achieved through the utilization of code. The system functions by adhering to predetermined criteria, autonomously implementing the terms of the agreement upon fulfillment of specified conditions. Distributed ledgers are responsible for the execution and maintenance of these contracts, utilizing blockchain technology to incorporate business logic into shared data [22]. Currently, the phrase “smart contract” primarily refers to automated computations that are carried out on blockchain systems. As an illustration, a directive could specify the transfer of 10 tokens to an individual on a predetermined date, contingent upon the fulfillment of a particular condition. Smart contracts in the Ethereum ecosystem are housed in contract accounts, which are only triggered when transactions are initiated to or from the respective account [23].

3. RESULTS AND DISCUSSION

The research presented in this study utilizes a blockchain network as the foundational infrastructure for the e-voting system. The blockchain network serves as the primary database for storing crucial election information, such as election titles, candidates, and the voter list. Each transaction involving the blockchain necessitates the utilization of a public-private key pair, which is assigned upon the creation of a blockchain account. To enhance user comfort, a server-side database is employed to hold the public-private keys. This eliminates the need for users to repeatedly input their public key when accessing the blockchain network.

Figure 3 the architecture of the proposed e-voting system. The initial step involves the organizer accessing a specifically designated webpage to initiate the establishment of a new election. The process entails inputting precise information, including the designation of the election, an enumeration of contenders, and the commencement and conclusion timings for the voting period. In addition, the individual responsible for coordinating the event enters the names and email addresses of qualified voters, which are subsequently saved within a server-based database. The aforementioned data is subsequently transmitted to a blockchain network, more precisely the Ethereum blockchain, so guaranteeing both transparency and security. During the second stage, voters get entry to the voting system’s webpage by inputting their email addresses. If the database of the system acknowledges the email as being registered, a distinct link is generated and thereafter dispatched to the corresponding email address. The provided hyperlink grants users access to the voting procedure. Voters can securely choose their chosen candidate. Following the conclusion of the voting procedure, individuals can access the instantaneous and unmodifiable election outcomes, hence enhancing the reliability and assurance of the e-voting system.

3.1. System communication protocol

The suggested system design incorporates many communication protocols for facilitating interactions inside the system, namely representational state transfer application programming interface (REST API) [24], JSON-RPC [25], and The peer-to-peer protocol (P2P) protocol [26]. The facilitation of communication between the computer of the organizer and the voters on the frontend server of the system is achieved through the utilization of the REST API protocol. Likewise, the communication between the frontend server and the external database is facilitated through the utilization of the REST API protocol. The communication between the front end and the smart contract is established via JSON-RPC. The exchange of information among nodes inside the blockchain network is facilitated using a peer-to-peer protocol. Individuals who choose to obtain election data stored on the blockchain may establish a direct connection to the smart contract by linking their computer to one of the nodes.

In this section, we present Figure 4 which illustrates the communication protocol employed in blockchain-based e-voting systems. The proposed system design incorporates the utilization of diverse communication protocols to facilitate different elements and interactions inside the system. Every protocol serves a distinct objective, guaranteeing seamless and protected communication among the diverse constituents of an e-voting system. The following is a comprehensive analysis of the function and significance of each protocol within the system. The REST API protocol is a standardized set of rules and guidelines that govern the communication and interaction between clients and servers in a RESTful architecture. To facilitate communication across many components, such as the primary computing system, the frontend server, and an external database. The host computer establishes communication with the system frontend through the utilization of the REST API. The present protocol facilitates the transmission of election particulars from organizers to a server in a standardized format. The frontend server utilizes the REST API for communication with the external database. This system enables the secure and efficient transmission and retention of voter data and election particulars. The JSON-RPC protocol facilitates the communication between front-end servers and smart contracts that are implemented on the Ethereum network. The P2P is responsible for facilitating and regulating the exchange of information and communication among nodes within a blockchain network.

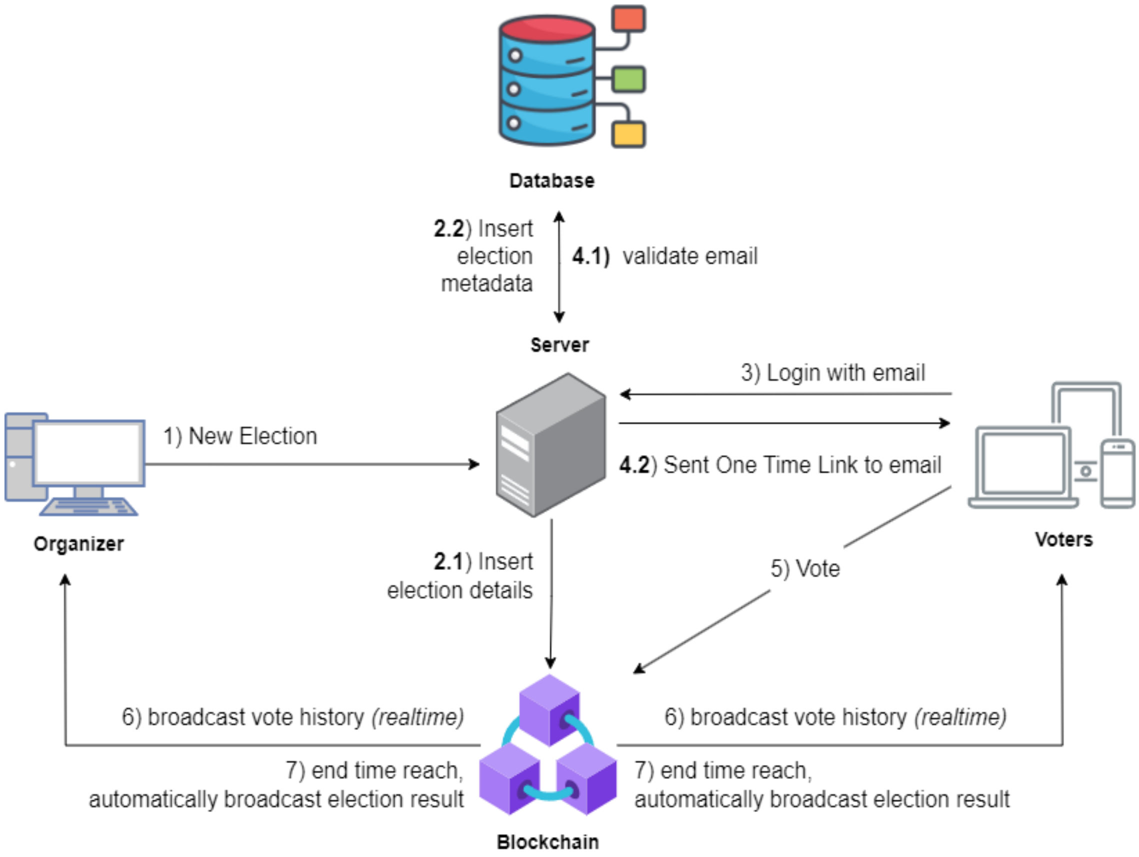

Database
2.2) Insert election metadata
4.1) validate email
Server
3) Login with email
4.2) Sent One Time Link to email
1) New Election
Organizer
Voters
2.1) Insert election details
5) Vote
6) broadcast vote history (realtime)
6) broadcast vote history (realtime)
7) end time reach, automatically broadcast election result
7) end time reach, automatically broadcast election result
Blockchain

Figure 3. The architecture of the proposed e-voting system

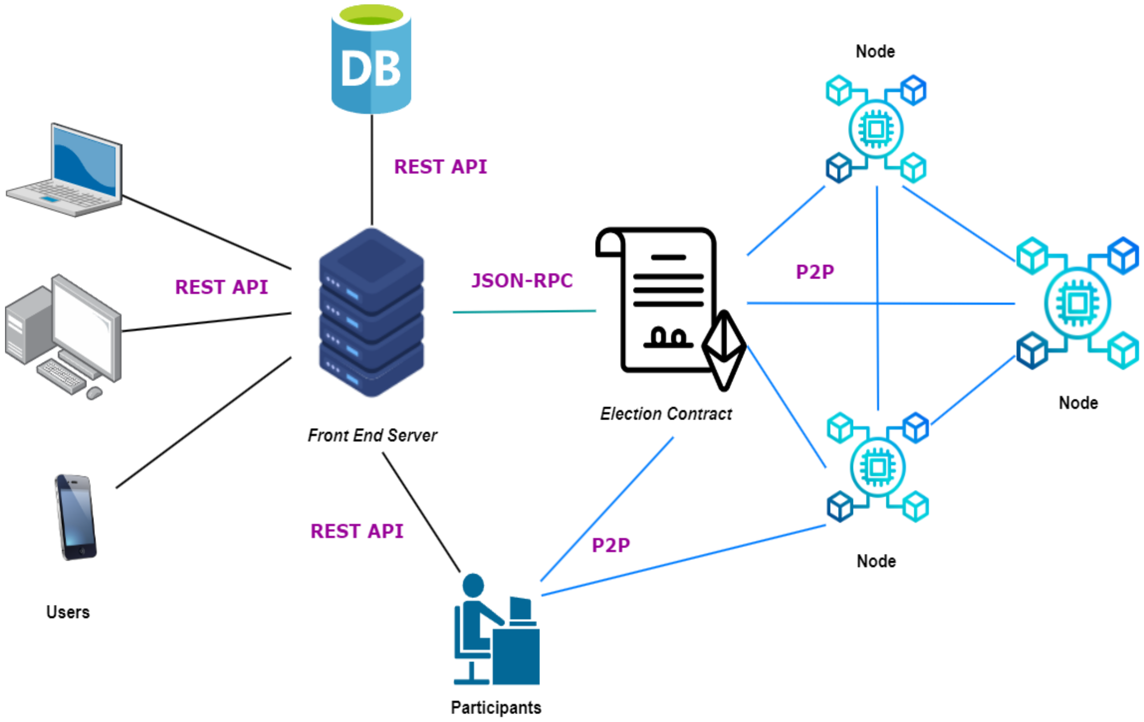
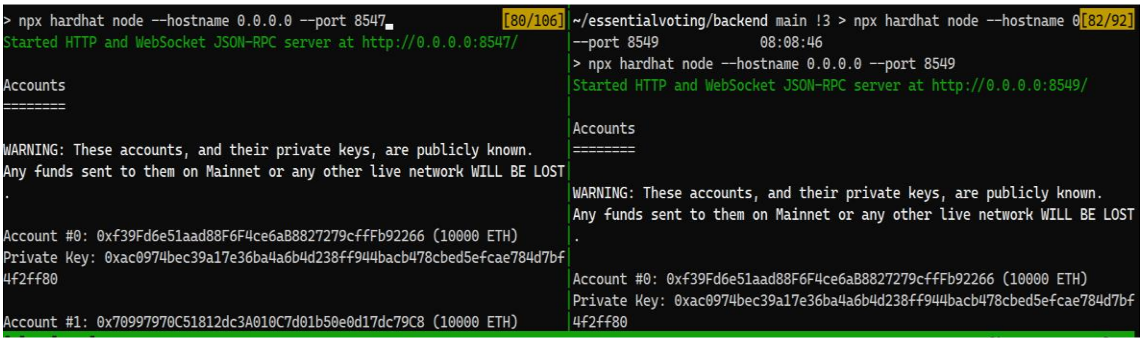


Figure 4. Blockchain e-voting communication protocol

3.2. Essential voting contract

The “essential voting contract” is a programmable contract designed to facilitate the establishment of elections on a blockchain network. Furthermore, it assumes the responsibility of overseeing the process of recording voter preferences and aggregating votes at the culmination of the electoral event. The smart contract has been deployed onto the Ethereum network, and for this research, the blockchain is operated using Hardhat as the chosen tool. Blockchain nodes serve as interconnected computers inside the blockchain network, facilitating the exchange of block data. Additionally, these nodes are responsible for validating requests to input data into the blockchain. The frontend application establishes a connection with one of the blockchain nodes, enabling it to have access to voting smart contracts. This study involves the utilization of four locally-operating nodes, employing the Hardhat tool for the purpose. Each instance of data insertion or retrieval in the blockchain will be meticulously documented in the transaction log of all active nodes.

Figure 5 illustrates the operation of four localized blockchain nodes, elucidating the integration of the voting system frontend application with a singular node within the blockchain network. This connection facilitates the ability of front-end applications to access and engage with voting smart contracts that have been installed on the blockchain. This smart contract facilitates secure and transparent voting and retrieval of election results for users. This study employs Hardhat, a development environment designed for Ethereum, to establish four local nodes that replicate the operational characteristics of an actual blockchain network. The utilization of Hardhat enables development teams to conduct testing and development activities of their voting system within a regulated setting, before its deployment on an authentic blockchain network. Each transaction, regardless of whether it involves adding new data or retrieving existing data from the blockchain, is meticulously documented in the log of every operational node. The utilization of a transparent and unalterable ledger enhances the security and transparency of the voting mechanism, guaranteeing the validity of each vote and enabling the verification of election outcomes by anyone granted access to the blockchain network. Transparency and accountability in the voting process are enhanced through the comprehensive recording of each transaction at every node, hence safeguarding the integrity and fairness of elections.



```
> npx hardhat node --hostname 0.0.0.0 --port 8547                 [80/106]
Started HTTP and WebSocket JSON-RPC server at http://0.0.0.0:8547/

Accounts
========

WARNING: These accounts, and their private keys, are publicly known.
Any funds sent to them on Mainnet or any other live network WILL BE LOST
.

Account #0: 0xf39Fd6e51aad88F6F4ce6aB8827279cffFb92266 (10000 ETH)
Private Key: 0xac0974bec39a17e36ba4a6b4d238ff944bacb478cbed5efcae784d7bf
4f2ff80

Account #1: 0x70997970C51812dc3A010C7d01b50e0d17dc79C8 (10000 ETH)
```

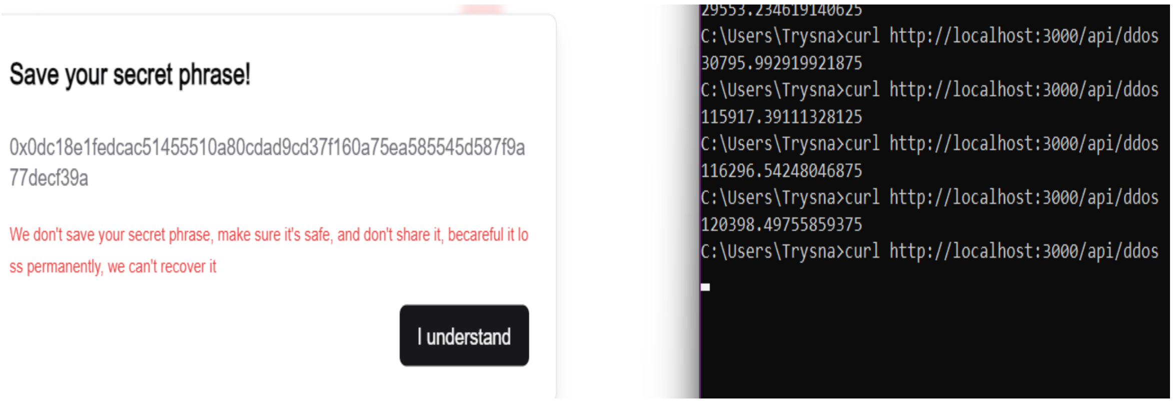
```
~/essentialvoting/backend main !3 > npx hardhat node --hostname 0[82/92]
--port 8549              08:08:46
> npx hardhat node --hostname 0.0.0.0 --port 8549
Started HTTP and WebSocket JSON-RPC server at http://0.0.0.0:8549/

Accounts
========

WARNING: These accounts, and their private keys, are publicly known.
Any funds sent to them on Mainnet or any other live network WILL BE LOST
.

Account #0: 0xf39Fd6e51aad88F6F4ce6aB8827279cffFb92266 (10000 ETH)
Private Key: 0xac0974bec39a17e36ba4a6b4d238ff944bacb478cbed5efcae784d7bf
4f2ff80
```

Figure 5. Running four local blockchain nodes

3.3. Testing attacks on the system

During the course of this experiment, a deliberate assault was executed on the blockchain technology to ascertain the robustness and safeguard the integrity of the system under development. The utilized method of attack is commonly referred to as denial of service (DoS) [27]. The objective of the assault would involve inundating the system with a high volume of requests to generate a large number of votes simultaneously, to impede users’ ability to initiate new electoral processes. To streamline the simulation process, the attack script is transformed into an endpoint that will be invoked.

In this section, we present the results of conducting an attack test on the system that was designed. The test was performed to evaluate the system’s vulnerability to potential attacks. The findings from this test are illustrated in Figure 6. In the given scenario, an assault is carried out with a frequency of 160 demands per second. The assault was orchestrated by the organizer to instigate a new election. Despite the persistent assault, the organizers can effectively institute fresh elections, and voters retain the capacity to exercise their right to vote. This exemplifies the system’s ability to withstand cyber attacks by maintaining its core functionalities, enabling the continuation of elections even in suboptimal conditions. The system’s capacity to endure such attacks guarantees the preservation and uninterrupted operation of the voting process, instilling trust in the dependability and safeguarding of the e-voting system.



Save your secret phrase!

0x0dc18e1fedcac51455510a80cdad9cd37f160a75ea585545d587f9a77decf39a

We don't save your secret phrase, make sure it's safe, and don't share it, becareful it loss permanently, we can't recover it

```
29553.234619140625
C:\Users\Trysna>curl http://localhost:3000/api/ddos
30795.992919921875
C:\Users\Trysna>curl http://localhost:3000/api/ddos
115917.39111328125
C:\Users\Trysna>curl http://localhost:3000/api/ddos
116296.54248046875
C:\Users\Trysna>curl http://localhost:3000/api/ddos
120398.49755859375
C:\Users\Trysna>curl http://localhost:3000/api/ddos
```

Figure 6. Attack test on the designed system

4. CONCLUSION

This research presents a significant improvement in voting methods by introducing a blockchain-based e-voting system. Traditional paper-based voting has been problematic due to costs, inaccuracies, and vulnerability to tampering. E-voting offers flexibility but faces concerns about security and transparency. The new system addresses these issues by incorporating blockchain technology, ensuring secure, and transparent voting. Features include secure election data storage, public-private key pairs, a server-side database, various communication protocols, and a smart contract framework. This makes the system secure, convenient, and reliable. It has undergone extensive testing, including addressing issues like timestamp discrepancies during voting windows. The system is particularly suitable for small to medium-scale elections, offering enhanced security through blockchain's network-based data validation. It stands out for its openness, allowing real-time access to election logs, thus fostering trust. The development and refinement of this system could revolutionize global elections, prioritizing security, transparency, and efficiency.

REFERENCES

[1] C. L. Brown, D. Raza, and A. D. Pinto, "Voting, health and interventions in healthcare settings: a scoping review," *Public Health Reviews*, vol. 41, no. 1, p. 16, Dec. 2020, doi: 10.1186/s40985-020-00133-6.

[2] A. Khan, J. Bhaisare, K. Chandekar, and A. Lichade, "Online Voting and Information Management," *International Journal of Advanced Research in Science, Communication and Technology*, pp. 514–517, Dec. 2022, doi: 10.48175/IJARSCT-7717.

[3] O. Daramola and D. Thebus, "Architecture-Centric Evaluation of Blockchain-Based Smart Contract E-Voting for National Elections," *Informatics*, vol. 7, no. 2, p. 16, May 2020, doi: 10.3390/informatics7020016.

[4] T. M. Roopak and R. Sumathi, "Electronic Voting based on Virtual ID of Aadhar using Blockchain Technology," in *2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)*, IEEE, Mar. 2020, pp. 71–75, doi: 10.1109/ICIMIA48430.2020.9074942.

[5] M. Sholeh, E. Y. Talahaturuson, M. Rizqi, and A. B. Gumelar, "Designing an Ethereum-based Blockchain for Tuition Payment System using Smart Contract Service," *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 6, no. 2, pp. 275–280, Apr. 2022, doi: 10.29207/resti.v6i2.3917.

[6] U. Jafar, M. J. A. Aziz, and Z. Shukur, "Blockchain for Electronic Voting System—Review and Open Research Challenges," *Sensors*, vol. 21, no. 17, p. 5874, Aug. 2021, doi: 10.3390/s21175874.

[7] N. Bore *et al.*, "On Using Blockchain Based Workflows," in *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, IEEE, May 2019, pp. 112–116, doi: 10.1109/BLOC.2019.8751446.

[8] A. K. Goel, A. Rai, A. Narain, A. Richard, and K. Kumar, "Trusted Vote: Reorienting eVoting using Blockchain," in *2022 Sixth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, IEEE, Nov. 2022, pp. 129–138, doi: 10.1109/I-SMAC55078.2022.9987301.

[9] R. AlAbri, A. K. Shaikh, S. Ali, and A. H. Al-Badi, "Designing an E-Voting Framework Using Blockchain Technology," *International Journal of Electronic Government Research*, vol. 18, no. 2, pp. 1–29, Mar. 2022, doi: 10.4018/IJEGR.298203.

[10] J. Cano-Benito, A. Cimmino, and R. Garcia-Castro, "Toward the Ontological Modeling of Smart Contracts: A Solidity Use Case," *IEEE Access*, vol. 9, pp. 140156–140172, 2021, doi: 10.1109/ACCESS.2021.3115577.

[11] M. Johnson, M. Jones, M. Shervey, J. T. Dudley, and N. Zimmerman, "Building a Secure Biomedical Data Sharing Decentralized App (DApp): Tutorial," *Journal of Medical Internet Research*, vol. 21, no. 10, p. e13601, Oct. 2019, doi: 10.2196/13601.

[12] L. Besancon, C. F. Da Silva, P. Ghodous, and J.-P. Gelas, "A Blockchain Ontology for DApps Development," *IEEE Access*, vol. 10, pp. 49905–49933, 2022, doi: 10.1109/ACCESS.2022.3173313.

[13] Z. Yang, L. Mao, B. Yan, J. Wang, and W. Gao, "Performance analysis and prediction of asymmetric two-level priority polling system based on BP neural network," *Applied Soft Computing*, vol. 99, p. 106880, Feb. 2021, doi: 10.1016/j.asoc.2020.106880.

[14] B. A. S., "Token Authentication based Election System with AI BOT," *International Journal for Research in Applied Science and Engineering Technology*, vol. 7, no. 3, pp. 288–295, Mar. 2019, doi: 10.22214/ijraset.2019.3051.

[15] A. Shojaei, I. Flood, H. I. Moud, M. Hatami, and X. Zhang, "An Implementation of Smart Contracts by Integrating BIM and Blockchain," in *Proceedings of the Future Technologies Conference (FTC) 2019*, 2020, pp. 519–527, doi: 10.1007/978-3-030-32523-7_36.

[16] R. F. Hayat, S. Aurangzeb, M. Aleem, G. Srivastava, and J. C.-W. Lin, “ML-DDoS: A Blockchain-Based Multilevel DDoS Mitigation Mechanism for IoT Environments,” *IEEE Transactions on Engineering Management*, pp. 1–14, 2022, doi: 10.1109/TEM.2022.3170519.

[17] C. Destri, “Compelled Turnout and Democratic Turnout: Why They Are Different,” *Political Studies*, Jan. 2023, doi: 10.1177/00323217221148038.

[18] C. Avgerou, S. Masiero, and A. Poulymenakou, “Trusting e-voting amid experiences of electoral malpractice: The case of Indian elections,” *Journal of Information Technology*, vol. 34, no. 3, pp. 263–289, Sep. 2019, doi: 10.1177/0268396218816199.

[19] K. Nam, C. S. Dutt, P. Chathoth, and M. S. Khan, “Blockchain technology for smart city and smart tourism: latest trends and challenges,” *Asia Pacific Journal of Tourism Research*, vol. 26, no. 4, pp. 454–468, Apr. 2021, doi: 10.1080/10941665.2019.1585376.

[20] A. A. Monrat, O. Schelen, and K. Andersson, “A Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunities,” *IEEE Access*, vol. 7, pp. 117134–117151, 2019, doi: 10.1109/ACCESS.2019.2936094.

[21] R. Yang *et al.*, “Public and private blockchain in construction business process and information integration,” *Automation in Construction*, vol. 118, p. 103276, Oct. 2020, doi: 10.1016/j.autcon.2020.103276.

[22] C. Wu, J. Xiong, H. Xiong, Y. Zhao, and W. Yi, “A Review on Recent Progress of Smart Contract in Blockchain,” *IEEE Access*, vol. 10, pp. 50839–50863, 2022, doi: 10.1109/ACCESS.2022.3174052.

[23] S. S. Kushwaha, S. Joshi, D. Singh, M. Kaur, and H.-N. Lee, “Systematic Review of Security Vulnerabilities in Ethereum Blockchain Smart Contract,” *IEEE Access*, vol. 10, pp. 6605–6621, 2022, doi: 10.1109/ACCESS.2021.3140091.

[24] G. O. Sorokin and D. Y. Syedin, “Development of REST API service for organizing information interaction of software systems through SMEV,” *Informatization and communication*, vol. 7, 2022, doi: 10.34219/2078-8320-2022-13-7-12-17.

[25] A. Newton and S. Hollenbeck, “JSON Responses for the Registration Data Access Protocol (RDAP),” Mar. 2015, doi: 10.17487/rfc7483.

[26] B. Djamaa, M. R. Senouci, H. Bessas, B. Dahmane, and A. Mellouk, “Efficient and Stateless P2P Routing Mechanisms for the Internet of Things,” *IEEE Internet of Things Journal*, vol. 8, no. 14, pp. 11400–11414, Jul. 2021, doi: 10.1109/JIOT.2021.3053339.

[27] R. SaiSindhuTheja and G. K. Shyam, “An efficient metaheuristic algorithm based feature selection and recurrent neural network for DoS attack detection in cloud computing environment,” *Applied Soft Computing*, vol. 100, p. 106997, Mar. 2021, doi: 10.1016/j.asoc.2020.106997.

BIOGRAPHIES OF AUTHORS

Agus Tedyyana is a senior lecturer at the Politeknik Negeri Bengkalis, Bengkalis, Riau, Indonesia. He has an educational background in computer science. He has worked in education as a lecturer since 2014. He has been continuing his Doctoral (Ph.D.) studies at the Universiti Utara Malaysia (UUM) Campus in Kedah Darul Aman, Malaysia, since early 2020. His research interests are in computer security. He can be contacted at email: agustedyyana@polbeng.ac.id.

Osman Ghazali is a Professor and the Dean of the School of Computing, Universiti Utara Malaysia. Osman holds a Ph.D. in Information Technology (Networking) from Awang Had Salleh Graduate School, Universiti Utara Malaysia (AHSGS). Prof. Osman Ghazali research interests are internetworking, cloud computing, and information security. He has more than 100 publications as refereed book chapters and refereed technical papers in journals and conferences. He is a senior member of the InterNetworks Research Laboratory (IRL). He is also a member of the IEEE and the ACM. He can be contacted at email: osman@uum.edu.my.

Tryo Asnafi is an alumnus student in Software Engineering from Politeknik Negeri Bengkalis. His research is centered on software engineering development. Presently, he actively engages in software engineering research while simultaneously maintaining a professional career as a software engineer, effectively bridging practical experience with academic insights. Currently, employed at Equnix Business Solutions, a company that espouses the principles of open source and open-minded approaches to business solutions. He can be contacted at email: tryoasnafi@gmail.com.

Onno W. Purbo graduated from the Department of Electrical Engineering, Bandung Institute of Technology, in 1987. In 1989, he completed his postgraduate education at McMaster University, Canada, in the field of semiconductor laser. Five years later, he received his Ph.D. from the University of Waterloo, Canada, in the field of integrated circuit technology for satellites, in November 2020, he received the Postel Service Award from the Internet Society. Postel Service Award was given to him for his outstanding contribution to the development of internet technology in Indonesia. He can be contacted at email: onno@indo.net.id.

Nur Ziadah Harun received the B.S. and M.Sc. degrees in Information Technology from the Faculty of Information Technology, Universiti of Utara Malaysia, in 2008 and 2012, respectively, and the Ph.D. degree in Quantum Cryptography from University Putra Malaysia. She is currently a lecturer with the Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia, since 2020. Her research interests focus on computer networks, quantum cryptography, and network security. She is a member of the IEEE Computer Society. She can be contacted at email: nurziadah@uthm.edu.my.

Faizal Riza is a seasoned network and server professional with over two decades of practical experience dating back to 1997. He is also pursuing his doctoral education at UPI YPTK Padang, with research interests focused on network security and robotics. Faizal’s dedication to advancing technology in these domains is evident through his commitment to bridging the gap between theory and practical application, making complex concepts accessible to a wide audience. He can be contacted at email: s3.faizal@gmail.com.